View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Elsevier - Publisher Connector

Theoretical Computer Science 88 (1991) 171–182
Elsevier

Note

Représentations des nombres réels par développements en base entière et complexité

Salah Labhalla

Département de Mathématiques, Université de Marrakech, Bd de Safi. BP S 15, Marrakech, Maroc, ou Département d'Informatique Université de Caen 14000 Caen, France

Henri Lombardi

UFR des Sciences et Techniques, Laboratoire de Mathématiques, Universite de Franche-Comté, 25030 Besancon Cedex, France

Communicated by D. Perrin
Received September 1990
Revised February 1991

Abstract

Labhalla S. and H. Lombardi, Représentations des nombres réels par developpements en base entière et complexité, Theoretical Computer Science 88 (1991) 171–182.

In this paper, we are concerned with the use of representation in basis β for real numbers in the computational theory of recursive analysis. The main results state:
- the existence of real numbers of low complexity in each representation of basis β but of arbitrarily high complexity in the Dedekind representation.
- the existence of a sequence of low complexity in each representation in basis β but which is not a recursive sequence in the Dedekind representation.

These questions were already raised by Mostowski in 1957.

Résumé

Labhalla S. and H. Lombardi, Représentations des nombres réels par developpements en base entière et complexité, Theoretical Computer Science 88 (1991) 171–182.

Nous étudions dans cet article la représentation des nombres réels en base β du point de vue de la théorie de la complexité pour l'analyse récursive. Les principaux résultats établissent:
- l'existence de nombres réels de faible complexité en toute représentation en base β mais de complexité arbitrairement grande dans la représentation par coupures de Dedekind.
- l'existence d'une suite de réels qui est de faible complexité en toute représentation en base β mais qui n'est pas récursive dans la représentation par coupures de Dedekind.

Ces questions avaient séjà été soulevées par Mostowski en 1957.

0304-3975/91/$03.50 © 1991—Elsevier Science Publishers B.V.

Introduction

La notion de réel récursif a été introduite par Turing en 1936 [7], et étudiée en détail, notamment par Specker [6] et Rice [5]. Plus récemment, Ko [2] a introduit et étudié la notion de complexité concernant différentes représentations d'un nombre réel (les représentations via les suites de Cauchy, les développements dyadiques et les coupures de Dedekind).

Dans [3], nous avons précisé les notations $\mathbb{R}_{\mathrm{CONV}}$ et $\mathbb{R}_{\mathrm{CUT}}$ de Ko (correspondant aux suites de Cauchy et aux coupures de Dedekind) et également défini les ensembles $\mathbb{R}_{\mathrm{CONT}}$ et $\mathbb{R}_{\mathrm{MIR}}$ correspondant aux représentations en fractions continues et via des mesures d'irrationalité.

Dans cet article, qui est un prolongement de [3], nous étudions des présentations des nombres réels associées aux coupures de Dedekind et à diverses présentations des développements en base β fixée ou arbitraire (présentations que nous notons $\mathbb{R}_{\mathrm{CUT}+}$, $\mathbb{R}_{\mathrm{Base1},\beta}$, $\mathbb{R}_{\mathrm{Base2},\beta}$, $\mathbb{R}_{\mathrm{Base}}$) en introduisant le point de vue des fonctionnelles récursives. Nous montrons que $\mathbb{R}_{\mathrm{CUT}+}$ et $\mathbb{R}_{\mathrm{Base}}$ ($\mathbb{R}_{\mathrm{Base1},\beta}$ et $\mathbb{R}_{\mathrm{Base2},\beta}$) sont des représentations $\mathscr{P}$-équivalentes de $\mathbb{R}$. Nous précisions en outre les relations entre $\mathbb{R}_{\mathrm{Base2},\beta}$ et $\mathbb{R}_{\mathrm{Base2},\beta'}$ (β et β' deux entiers).

En combinant avec les résultats de [3], nous obtenons la chaîne de $\mathscr{P}$-fonctionnelles dans les cas suivants pour représenter l'identité de $\mathbb{R}$:

$$\mathbb{R}_{\mathrm{CONT}} \to \mathbb{R}_{\mathrm{MIR}} \to \mathbb{R}_{\mathrm{CUT}} \to \mathbb{R}_{\mathrm{CUT}+} \;\equiv\; \mathbb{R}_{\mathrm{Base}} \to \mathbb{R}_{\mathrm{Base1},\beta} \;\equiv\; \mathbb{R}_{\mathrm{Base2},\beta} \to \mathbb{R}_{\mathrm{CONV}},$$

et aucune des flèches $\to$ dans la ligne ci-dessus n'est une $\mathscr{P}$-équivalence.

L'impossibilité d'obtenir certaines fonctions sous forme de fonctionnelles récursives est en général facile à établir. Cette impossibilité peut souvent être explicitée et renforcée en termes de complexité:

- il existe des points de faibles complexité ayant une image de complexité arbitrairement grande.
- il existe une suite de faible complexité dont l'image est une suite non récursive.

Nous obtenons, pour une classe de complexité en temps $\mathscr{C}$ arbitrairement grande, les non-inclusions suivantes:

$$\mathbb{R}_{\mathrm{Base2},\beta}(\mathscr{C}) \not\supseteq \mathbb{R}_{\mathrm{Base2},\beta'}(\mathbf{DTIME}(\mathrm{O}(n^2)))$$

s'il existe un premier divisant β ne divisant pas β',

$$\mathbb{R}_{\mathrm{Base}}(\mathscr{C}) \not\supseteq \bigcap_{\beta} \mathbb{R}_{\mathrm{Base2},\beta}(\mathbf{DTIME}(\mathrm{O}(n^3)))$$

De même, nous construisons une $\mathbf{DTIME}(\mathrm{O}(n^2))$-suite dans $\mathbb{R}_{\mathrm{Base2},\beta'}$ qui n'est pas récursive dans $\mathbb{R}_{\mathrm{Base2},\beta}$ (s'il existe un premier divisant β ne divisant pas β') et une suite qui est $\mathbf{DTIME}(\mathrm{O}(n^2))$ dans chaque $\mathbb{R}_{\mathrm{Base2},\beta}$ mais qui n'est pas récursive dans $\mathbb{R}_{\mathrm{Base}}$. Nous répondons ainsi, de manière précise, à des questions posées par Mostowski [4].

1. Notations et définitions

On désignera par $\mathscr{C}$ une classe de complexité, ou la classe des fonctions récursives; par $\mathbb{N}_1$ l'ensemble des entiers naturels en représentation unaire; par $\mathbb{N}$ l'ensemble des entiers naturels en représentation binaire; par $\mathbb{Q}$ l'ensemble des rationnels en représentation binaire; par **LINTIME** la complexité en temps linéaire (déterministe) et enfin par $\mathscr{P}$ la complexité en temps polynomial.

Nous notons $[x]$ la partie entière du réel x. Pour un entier n, nous notons $\lg(n)$ la longueur de son écriture en binaire.

$$\text{Enfin, nous notons } \mathbf{DTIME}(\mathrm{O}(n^{k+})) := \bigcup_b \mathbf{DTIME}(\mathrm{O}(n^k \cdot \lg^b(n))).$$

La classe $\mathbf{DTIME}(\mathrm{O}(n^{1+}))$ intervient dans les calculs arithmétiques en entiers.

1.1. Fonctionnelle uniformément en temps polynomial

Nous considérons des fonctionnelles récursives définissables au moyen de Machines de Turing à Oracles, ou ce qui revient au même, définissables dans un langage de programmation ordinaire avec en outre des instructions correspondant au questionnement des oracles. Ces oracles donnent une réponse discrète (du type entier naturel) à une question discrète. Dans ce cadre, les notions de fonctionnelles récursives, ou uniformément primitives récursives sont bien connues dans la littérature. Le cas des classes de complexité en temps pour les fonctionnelles où les oracles ne donnent qu'un nombre fini à priori de réponse (par exemple "oui", ou "non"), est également bien connu. Nous aurons en outre besoin d'une notion générale de fonctionnelle uniformément en temps polynomial. Nous ne proposerons pas de définition, mais nous faisons les 2 remarques suivantes:

primo: les fonctionnelles en temps polynomial que nous construisons sont toujours du type très simple qui suit: elles peuvent être calculées par un programme sans aucune boucle dont les instructions de base sont les suivantes:

- des instructions $N := f(M_1, M_2, \ldots, M_k)$ où f est une fonction calculable en temps polynomial,
- des instructions "oracle": $N := g(M_1, M_2, \ldots, M_j)$ où g désigne un oracle,
- des instructions "liste des L premières valeurs d'un oracle":

$$N := \text{nombre codant la liste des valeurs } [h(0), h(1), \ldots, h(L)],$$

où h désigne un oracle et l'entrée L de l'instruction est en unaire.

secundo: nous adoptons le critère négatif suivant: s'il existe une suite calculable en temps polynomial, $(u_n)_{n \in \mathbb{N}_1}$, telle que $(F(u_n))_{n \in \mathbb{N}_1}$ soit une suite non calculable en temps polynomial, alors la fonctionnelle F n'est sûrement pas (uniformément) calculable en temps polynomial.

Il nous semble clair que toute définition raisonnable de la notion de fonctionnelle uniformément calculable en temps polynomial doit être cohérente avec le "primo" et le "secundo" ci-dessus.

1.2. Différentes représentations de l'ensemble des réels

Nous rappelons tout d'abord les définitions des ensembles $\mathbb{R}_{\mathrm{CONV}}$ et $\mathbb{R}_{\mathrm{CUT}}$ correspondant aux représentations par suites de Cauchy et coupures de Dedekind, telles que nous les avons données dans [3].

Définition 1 (*Réels à la Cauchy*). Nous définissons $\mathbb{R}_{\mathrm{CONV}}$ comme la partie de $\mathbb{Q}^{\mathbb{N}_1}$ formée des suites $(x_n)_{n\in\mathbb{N}_1}$ de rationnels vérifiant la condition: $|x_n - x_{n+1}| \leqslant 1/2^{n+1}$. La suite (x_n) représente le nombre réel $x = \lim x_n$.

Définition 2 (*Réels à la Dedekind*). Nous définissons $\mathbb{R}_{\mathrm{CUT}}$ comme une partie de $\mathbb{Z}\times\{-1, 0, +1\}^{\mathbb{Q}}$. Un élément (z, t) de $\mathbb{Z}\times\{-1, 0, +1\}^{\mathbb{Q}}$ est dans $\mathbb{R}_{\mathrm{CUT}}$ si et seulement si les conditions suivantes sont vérifiées (q et q' sont des rationnels):
(i) la fonction t est croissante et elle prend au plus une fois la valeur 0,
(ii) $\forall q\ (t(q) > 0 \Rightarrow \exists q' < q,\ t(q') > 0)$,
$\forall q (t(q) < 0 \Rightarrow \exists q' > q',\ t(q') < 0)$,
(iii) $t(z) < 0 < t(z+2)$.
Le test t représente l'unique nombre réel x pour lequel: $\forall q$ signe$(q - x) = t(q)$.

Nous définissons maintenant les ensembles $\mathbb{R}_{\mathrm{CUT}+}$, $\mathbb{R}_{\mathbf{Base1},\beta}$, $\mathbb{R}_{\mathbf{Base2},\beta}$ et $\mathbb{R}_{\mathbf{Base}}$ attachés à chacune des représentations des nombres réels que nous étudions plus particulièrement dans cet article. Dans toute la suite β designe un entier $\geqslant 2$.

Concernant les coupures de Dedekind, outre le test $t_x(q) = \text{signe}(q - x)$, on peut considérer un test $t_x^+(q)$ qui ne prend que les valeurs -1 ou $+1$ selon que $q \leqslant x$ ou $x < q$. Notons que si n est entier: $(t_x^+(n) = -1$ et $t_x^+(n+1) = +1) \Leftrightarrow [x] = n$. Cela conduit à définir un ensemble $\mathbb{R}_{\mathrm{CUT}+}$ comme une partie convenable de $\mathbb{Z}\times\{-1, +1\}^{\mathbb{Q}}$.[1]

Définition 3. (*réels à la Dedekind, variante*). Nous définissons $\mathbb{R}_{\mathrm{CUT}+}$ comme une partie de $\mathbb{Z}\times\{-1, +1\}^{\mathbb{Q}}$. Un élément (z, t) de $\mathbb{Z}\times\{-1, +1\}^{\mathbb{Q}}$ est dans $\mathbb{R}_{\mathrm{CUT}+}$ si et seulement si les conditions suivantes sont vérifiées (q et q' sont des rationnels):
(i) la fonction t est croissante,
(ii) $\forall q\ (t(q) = 0 \Rightarrow \exists q' < q,\ t(q') > 0)$,
(iii) $t(z) < 0 < t(z+2)$.

Définition 4 (*réels par développement en base entière fixée*). Nous définissons $\mathbb{R}_{\mathbf{Base1},\beta}$ comme une partie de $\mathbb{Z}\times\{0, 1, 2, \ldots, \beta-1\}^{\mathbb{N}_1}$. Un élément $(z, (c_n)_{n\in\mathbb{N}_1})$ de $\mathbb{Z}\times\{0, 1, 2, \ldots, \beta-1\}^{\mathbb{N}_1}$ est dans $\mathbb{R}_{\mathbf{Base1},\beta}$ si et seulement si la condition suivante est

[1] Dans [3] nous avons considéré l'ensemble $\mathbb{R}_{\mathrm{CUT}-}$ basé sur le test symétrique du précédent.

vérifiée: $\forall m\ \exists n > m,\ c_n \neq \beta - 1$. Le couple $(z, (c_n))$ représente le nombre réel x défini par

$$x = z + \sum_{i=0}^{\infty} \frac{c_i}{\beta^{i+1}}.$$

Remarque 1. Pour $x \geqslant 0$, $(z, (c_n))$ est le développement classique de x en base β.

Définition 5 (*réels par développement en base entière fixée, variante*). Nous définissons $\mathbb{R}_{\mathrm{Base2},\beta}$ comme une partie de $\mathbb{Z}^{\mathbb{N}_1}$ formée des suites $(u_n)_{n\in\mathbb{N}_1}$ d'entiers vérifiant les conditions:

(i) $\beta u_n \leqslant u_{n+1} \leqslant \beta u_n + \beta - 1$,

(ii) $\forall m\ \exists n > m,\ u_{n+1} - \beta u_n \neq \beta - 1$.

La suite (u_n) représente le réel x: $x = \lim(u_n/\beta^n)$, et on a $u_n = [\beta^n x]$.

Définition 6 (*réels par développement dans chaque base entière*). Nous définissons $\mathbb{R}_{\mathrm{Base}}$ comme une partie de $\mathbb{Z}^{\mathbb{N}^*}$. Un élément v de $\mathbb{Z}^{\mathbb{N}^*}$ est dans $\mathbb{R}_{\mathrm{Base}}$ si et seulement si les conditions suivantes sont vérifiées:

(i) $\forall \beta\ \forall n\ \beta v(\beta^n) \leqslant v(\beta^{n+1}) \leqslant \beta v(\beta^n) + \beta - 1$,

(ii) $\forall \beta\ \forall n\ \exists p > n,\ v(\beta^{p+1}) - \beta v(\beta^p) \neq \beta - 1$,

(iii) $\forall \beta, \beta'\ \lim[v(\beta^n)/\beta^n] = \lim[v(\beta'^n)/\beta'^n]$.

Sous ces conditions, v représente l'unique réel x vérifiant $\forall \beta\ v(\beta) = [\beta x]$.

Définitions et notations 7. Pour chacun des ensembles $\mathbb{R}_X$ précédemment définis, on désigne par $\mathbb{R}_X(\mathscr{C})$ l'ensemble des éléments de $\mathbb{R}_X$ qui sont dans la classe $\mathscr{C}$. Et on dit qu'un nombre réel x est dans $\mathbb{R}_X(\mathscr{C})$ pour signifier qu'il peut être défini par un élément de $\mathbb{R}_X(\mathscr{C})$. De même, une suite $(x_m)_{m\in\mathbb{N}_1}$ de réels est appelée une $\mathscr{C}$-suite dans $\mathbb{R}_{\mathrm{CONV}}$ si on connaît une suite $(x_{m,n}): \mathbb{N}_1 \times \mathbb{N}_1 \to \mathbb{Q}$ de complexité $\mathscr{C}$ vérifiant la condition

$$|x_m - x_{m,n}| \leqslant 1/2^n.$$

On définirait également, pour chacun des ensembles $\mathbb{R}_X$ précédemment définis, les $\mathscr{C}$-suites dans $\mathbb{R}_X$ de manière analogue aux $\mathscr{C}$-suites dans $\mathbb{R}_{\mathrm{CONV}}$.

Lorsque $\mathscr{C}$ désigne la classe de toutes les fonctions récursives, on retrouve les notions classiques de suites récursives de réels au sens de Cauchy, de Dedekind, etc.

2. Comparaison du point de vue des fonctionnelles récursives

Dans [3], nous avons également défini les ensembles $\mathbb{R}_{\mathrm{CONT}}$ et $\mathbb{R}_{\mathrm{MIR}}$ correspondant aux représentations en fractions continues et via des mesures d'irrationalité, et nous avons notamment obtenu des $\mathscr{P}$-fonctionnelles représentant l'identité de $\mathbb{R}$ pour

$$\mathbb{R}_{\mathrm{CONT}} \to \mathbb{R}_{\mathrm{MIR}} \to \mathbb{R}_{\mathrm{CUT}} \to \mathbb{R}_{\mathrm{CONV}}.$$

Il est immédiat que l'on a des $\mathscr{P}$-fonctionnelles représentant l'identité de $\mathbb{R}$ pour

$$\mathbb{R}_{\text{Base}} \to \mathbb{R}_{\text{Base}2,\beta} \quad \text{et} \quad \mathbb{R}_{\text{CUT}} \to \mathbb{R}_{\text{CUT}+}.$$

Par ailleurs, nous démontrons ci-dessous que $\mathbb{R}_{\text{CUT}+}$ et $\mathbb{R}_{\text{Base}}$ ($\mathbb{R}_{\text{Base}1,\beta}$ et $\mathbb{R}_{\text{Base}2,\beta}$) sont deux présentations $\mathscr{P}$-équivalentes de $\mathbb{R}$. Enfin le même algorithme que celui donné pour $\mathbb{R}_{\text{CUT}} \to \mathbb{R}_{\text{CONV}}$ dans [3] fournit une $\mathscr{P}$-fonctionnelle de $\mathbb{R}_{\text{Base}2,\beta}$ vers $\mathbb{R}_{\text{CONV}}$. Tout ceci donne la chaîne de $\mathscr{P}$-fonctionnelles:

$$\mathbb{R}_{\text{CONT}} \to \mathbb{R}_{\text{MIR}} \to \mathbb{R}_{\text{CUT}} \to \mathbb{R}_{\text{CUT}+} \equiv \mathbb{R}_{\text{Base}} \to \mathbb{R}_{\text{Base}1,\beta} \equiv \mathbb{R}_{\text{Base}2,\beta} \to \mathbb{R}_{\text{CONV}}.$$

Il résulte de [3] et des résultats démontrés ci-dessous qu'aucune des flèches ($\to$) n'est une $\mathscr{P}$-equivalence.

Proposition 1. *Les deux présentations $\mathbb{R}_{\text{Base}}$ et $\mathbb{R}_{\text{CUT}+}$ de $\mathbb{R}$ sont $\mathscr{P}$-équivalentes.*

Preuve. Dans le sens $\mathbb{R}_{\text{CUT}+}$ vers $\mathbb{R}_{\text{Base}}$ on a plus précisément une **DTIME**($\mathrm{O}(n^2)$) fonctionnelle de $\mathbb{N}^* \times \mathbb{Z} \times \{-1, +1\}^{\mathbb{Q}}$ vers $\mathbb{Z}$ qui, restreinte à $\mathbb{N}^* \times \mathbb{R}_{\text{CUT}+}$, représente l'identité de $\mathbb{R}$, de $\mathbb{R}_{\text{CUT}+}$ vers $\mathbb{R}_{\text{Base}}$:

En effet, nous avons comme entrées un entier positif β et un entier z (x est sur l'intervalle $[z, z+2]$); et nous disposons d'un oracle t pour le réel x dans $\mathbb{R}_{\text{CUT}+}$. Une recherche par dichotomie parmi les entiers de βz à $\beta z + 2\beta$ permet de calculer $v(\beta) = [\beta x]$. Cette recherche nécessite au plus $\lg(2\beta)$ tests et, β étant écrit en binaire, se fait en temps $\mathrm{O}(n^2)$.

Dans le sens $\mathbb{R}_{\text{Base}}$ vers $\mathbb{R}_{\text{CUT}+}$ nous avons la $\mathscr{P}$-fonctionnelle uniforme qui fournit le test t à partir de v:

$$t(a/b) = \begin{cases} -1 & \text{si } v(b) \geqslant a, \\ +1 & \text{sinon.} \end{cases}$$

En effet: $a/b \leqslant x \Leftrightarrow a \leqslant bx \Leftrightarrow a \leqslant [bx]$.

NB: cette dernière fonctionnelle est sûrement uniformément **LINTIME** pour toute définition raisonnable de cette expression dans ce contexte. □

Remarque 2. Si A est une $\mathscr{P}$-partie dense de $\mathbb{Q}$, on peut définir une représentation $\mathbb{R}_{\text{CUT}+,A}$ de $\mathbb{R}$ où le réel x est représenté par $t^+_{x|A}$. Si on pose $A(\beta) = \{s \mid \beta^n;\ s \in \mathbb{Z},\ n \in \mathbb{N}\}$ on obtient comme à la proposition 1 que $\mathbb{R}_{\text{CUT}+,A(\beta)}$ et $\mathbb{R}_{\text{Base}2,\beta}$ sont des représentations $\mathscr{P}$-équivalentes de $\mathbb{R}$.

Proposition 2. *$\mathbb{R}_{\text{Base}1,\beta}$ et $\mathbb{R}_{\text{Base}2,\beta}$ sont deux représentations $\mathscr{P}$-équivalentes de $\mathbb{R}$.*

Preuve. Nous utilisons les égalités suivantes:

$$c_n = [\beta^{n+1} x] - \beta[\beta^n x], \quad n \geqslant 0,$$

$$u_n = c_n + \beta c_{n-1} + \cdots + \beta^n c_0 + \beta^{n+1} z,$$

$$c_n = u_{n+1} - \beta u_n, \quad z = u_0.$$

NB: Dans le sens $\mathbb{R}_{\mathrm{Base1},\beta} \to \mathbb{R}_{\mathrm{Base2},\beta}$ la fonctionnelle qui représente l'identité de $\mathbb{R}$ est dans $\mathbf{DTIME}(\mathrm{O}(n^2))$. Dans l'autre sens elle est sûrement uniformément **LINTIME** pour toute définition raisonnable de cette expression dans ce contexte. □

Proposition 3. *Si tout facteur premier de β divise β' alors il y a une $\mathscr{P}$-fonctionnelle de $\mathbb{R}_{\mathrm{Base2},\beta'}$ vers $\mathbb{R}_{\mathrm{Base2},\beta}$ qui représente l'identité de $\mathbb{R}$.*
Si il y a un facteur premier p de β qui ne divise pas β', il n'y a pas de fonctionnelle récursive du $\mathbb{R}_{\mathrm{Base2},\beta'}$ vers $\mathbb{R}_{\mathrm{Base2},\beta}$ qui représente l'identité de $\mathbb{R}$.

Preuve. (a) Pour certains entiers m et γ on a $\beta'^m = \gamma\beta$. Alors, $\beta'^{mn}x = \gamma^n\beta^n x$, donc, γ^n-étant entier, $[\beta^n x] = [[\beta'^{mn}x]/\gamma^n]$.

(b) Nous reprenons les notations $\mathbb{R}_{\mathrm{CUT}+,A}$ et $A(\beta)$ de la remarque 2. Si A est une partie dense de $\mathbb{Q}$ et $a \in \mathbb{Q} - A$, $t_x^+(a)$ ne dépend pas continûment de $t_{x|A}^+$. A fortiori il n'existe pas de fonctionnelle récursive dont la restriction à $\mathbb{R}_{\mathrm{CUT}+,A}$ calcule $t_x^+(a)$ à partir d'une représentation de x dans $\mathbb{R}_{\mathrm{CUT}+,A}$.

Puisque $1/p \notin A(\beta')$, $t_x^+(1/p)$ n'est pas donné par une fonctionnelle récursive à partir de la représentation de x dans $\mathbb{R}_{\mathrm{CUT}+,A(\beta')}$ donc pas non plus à partir de la représentation de x dans $\mathbb{R}_{\mathrm{Base2},\beta'}$. Mais $t_x^+(1/p)$ est donné dans la représentation de x dans $\mathbb{R}_{\mathrm{CUT}+,A(\beta)}$ donc est obtenu par une $\mathscr{P}$-fonctionnelle à partir de la présentation de x dans $\mathbb{R}_{\mathrm{Base2},\beta}$. Ceci prouve le résultat cherché. □

3. Points de faible complexité ayant une image de complexité arbitrairement grande

Dans la suite, nous utilisons un "lemme fondamental" pour construire des réels convenables. Rappelons tout d'abord une version en unaire du théorème de hiérarchie et un lemme sur les fonctions constructibles en temps.

Théorème de hiérarchie (en unaire). *Soient T_1 et T_2 deux fonctions récursives de $\mathbb{N}$ vers $\mathbb{N}^*$ vérifiant :*
- *T_1 est constructible en temps avec $T_1(n) \geqslant 2^n$,*
- *$T_2(n) \geqslant n$,*
- *$T_2(n) \cdot \log(T_2(n))/T_1(n)$ tend vers 0.*

Alors, il existe une partie A de $\mathbb{N}_1$ qui est dans $\mathbf{DTIME}(T_1(n))$ *mais pas dans* $\mathbf{DTIME}(T_2(n))$.

Lemme 1. (a) *Si S et T sont deux fonctions constructibles en temps croissantes $\geqslant 2n$, alors la composée de S et T est également constructible en temps.*
(b) *Si S est constructible en temps croissante $\geqslant 2n$, alors la fonction U construite par récurrence à partir de S:*

$$U(0) := a, \qquad U(n+1) := S(U(n))$$

est également constructible en temps.

La preuve du lemme se déduit immédiatement de la caractérisation des fonctions constructibles en temps (cf. par exemple [1, p. 44].

Théorème (caractérisation des fonctions constructibles en temps). *Soient* $\varepsilon > 0$ *et* f *une fonction telle que pour tout entier* $n, f(n) \geqslant (1+\varepsilon)\cdot n$. *Alors* f *est constructible en temps si et seulement si* f *est calculable en temps* $\mathrm{O}(f(n))$ (n *et* $f(n)$ *sont en unaire*).

Lemme fondamental. *Pour toute fonction récursive croissante* V *il existe une fonction* U *constructible en temps, et une partie* $\mathscr{A}$ *de* $\mathbb{N}_1$, *de fonction caractéristique* $\chi_{\mathscr{A}}$ *vérifiant:*
– $\chi_{\mathscr{A}}(n)$ *est calculable en temps* $U(n)$,
– $\chi_{\mathscr{A}}(n+1)$ *n'est pas calculable en temps* $V(U(n))$
(*autrement dit* $\mathscr{A} \in \mathbf{DTIME}(U(n))$ *mais* $1+\mathscr{A} \notin \mathbf{DTIME}(V(U(n)))$).

Preuve. On majore V par une fonction croissante W constructible en temps. Il suffit d'établir le lemme avec W. Soit U la fonction définie par

$$U(1) := 1; \qquad U(n+1) := 2^{W(U(n))}.$$

Alors, d'après le théorème de hiérarchie en unaire et le lemme 1, il existe une partie A de $\mathbb{N}_1$ reconnaissable en temps U mais pas en temps $\log_2(U)$ c.-à-d.: $\chi_A(n)$ est calculable en temps $U(n)$, mais $\chi_A(n+1)$ n'est pas calculable en temps $W(U(n))$. □

Dans la suite, nous aurons besoin du lemme suivant:

Lemme 2. *Soit* U *une fonction constructible en temps croissante vérifiant* $U(k+1) > 2U(k)$.
(a) *pour* $k < M$ *et* $k, M \in \mathbb{N}_1$ *la comparaison entre* $U(k)$ *et* M *est en temps* $\mathrm{O}(M)$.
(b) *pour* $M \in \mathbb{N}_1$ *la recherche du plus petit* k *tel que* $U(k) > M$ *est en temps* $\mathrm{O}(M)$.

Preuve. $U(k)$ est calculable en temps $c \cdot U(k)$ (où c est une constante).
(a) Programme: essayer de calculer $U(k)$ en $c \cdot M$ étapes au maximum.
– Si ça marche, on a $U(k)$ qu'on compare à M.
– Sinon, on sait que $U(k) > M$.
Le temps de calcul est majoré par $c' \cdot U(k)$ dans le premier cas (car M n'est pas nécessairement lu en entier) et par $c \cdot M$ dans le second cas.
(b) Comparer $U(i)$ et M en incrémentant i de 1 à chaque étape, selon l'algorithme du a). Le temps total de calcul est majoré par

$$c'(U(0) + U(1) + \cdots + U(k-1) + M) < c'(2U(k-1) + M) \leqslant 3c'M. \qquad \square$$

Théorème 1. *Si il existe un facteur premier* p *de* β *qui ne divise pas* β' *alors: pour toute fonction récursive* $S(n)$ *il existe un nombre réel* x *qui est dans* $\mathbb{R}_{\mathrm{Base2},\beta'}(\mathbf{DTIME}(\mathrm{O}(n^{1+})))$ *mais pas dans* $\mathbb{R}_{\mathrm{Base2},\beta}(\mathbf{DTIME}(S(n)))$.

Preuve. Soit T une fonction récursive croissante constructible en temps qui majore S. Soit $V(n) := T(2n)$, et U et $\mathscr{A}$ construits à partir de V comme dans le lemme fondamental. En particulier, $U(k+1) > 2U(k)$. Soit x défini par

$$x = \sum_{i=0}^{\infty} \frac{2\chi_{\mathscr{A}}(i) - 1}{p^{U(i)}}.$$

On pose:

$$d_k = \sum_{i=0}^{k} \frac{2\chi_{\mathscr{A}}(i) - 1}{p^{U(i)}}.$$

On a $d_k \in A(\beta)$, sa taille est majorée par $2U(k)$ et le signe de $x - d_k$ est donné par $\chi_{\mathscr{A}}(k+1)$, ce qui ce qui coûte asymptotiquement plus que $V(U(k)) > T(2U(k))$.

Ceci montre que $x \notin \mathbb{R}_{\mathrm{CUT}+, A(\beta)}(\mathbf{DTIME}(T(n)))$ et donc $x \notin \mathbb{R}_{\mathrm{Base}2, \beta}(\mathbf{DTIME}(T(n)))$. Démontrons maintenant que la suite $n \mapsto [\beta'^n x]$ (de $\mathbb{N}_1$ vers $\mathbb{Z}$) est dans $\mathbf{DTIME}(\mathrm{O}(n^{1+}))$. Soit c_0 tel que $p^{c_0} > \beta'$, et n_0 tel que $U(0) \leqslant 2 + 2c_0 n_0$.

Tout d'abord, pour tout entier $n \in \mathbb{N}_1$, $\geqslant n_0$, la recherche de l'entier $k(n) \in \mathbb{N}_1$ tel que

$$U(k) \leqslant 2 + 2c_0 n < U(k+1)$$

coûte un temps $\mathrm{O}(n)$ d'après le Lemme 2.

Alors $(d_{k(n)})$ (en tant que suite de rationnels écrits en base p) est dans $\mathbf{DTIME}(\mathrm{O}(n))$: en effet, une fois calculé k, le temps de calcul en base p de la somme ci-dessus est majoré par $c \cdot (U(1) + \cdots + U(k)) < 2 \cdot c \cdot U(k) < c' \cdot n$). On a de plus:

$$2\beta'^n p^{U(k)} < p^{1 + c_0 n + U(k)} < p^{U(k+1)}.$$

On a la majoration:

$$|x - d_{k(n)}| \leqslant \frac{2}{p^{U(k+1)}},$$

et par suite

$$|\beta'^n x - \beta'^n d_{k(n)}| \leqslant \frac{2\beta'^n}{p^{U(k+1)}} < \frac{1}{p^{U(k)}}.$$

Or $\beta'^n d_k$ est un rationnel irréductible de dénominateur $p^{U(k)}$, d'où $[\beta'^n x] = [\beta'^n d_{k(n)}]$. Enfin, le calcul de β'^n en base p, puis de la partie entière de $\beta'^n d_{k(n)}$, est dans $\mathbf{DTIME}(\mathrm{O}(n^{1+}))$ en utilisant les techniques de multiplication rapide des entiers. □

Théorème 2. *Pour toute fonction récursive $S(n)$ il existe un nombre réel x qui est dans $\bigcap_\beta \mathbb{R}_{\mathrm{Base}2, \beta}(\mathbf{DTIME}(\mathrm{O}(n^{2+})))$ mais pas dans $\mathbb{R}_{\mathrm{Base}}(\mathbf{DTIME}(S(n)))$.*

Preuve. Quoique un peu plus pénible, la preuve est essentiellement la même que pour le Théorème 1. Soit T une fonction récursive croissante constructible en temps qui majore S. Soit $V(n) := T(n^2)$, et U et $\mathscr{A}$ construits à partir de V comme dans le lemme fondamental. Il n'est pas restrictif de supposer qu'on a $U(k+1) > 3U(k)$ pour tout k.

Soit (p_i) une suite croissante (au sens large) **LINTIME** (i et p_i écrits en unaire) de nombres premiers tendant vers l'infini, avec $p_i \leqslant i+2$. Soit x défini par

$$x = \sum_{i=0}^{\infty} \frac{2\chi_{\mathscr{A}}(i)-1}{p_i^{U(i)}}.$$

On pose:

$$d_k = \sum_{i=0}^{k} \frac{2\chi_{\mathscr{A}}(i)-1}{p_i^{U(i)}}.$$

La taille de d_k est en $\mathrm{O}(\lg(k)\cdot U(k))$, et le signe de $x-d_k$ dépend de $\chi_{\mathscr{A}}(k+1)$, ce qui coûte asymptotiquement plus que $T(U(k)^2)$ donc plus que $T(c\cdot\lg(k)\cdot U(k))$.
Ainsi $x \notin \mathbb{R}_{\mathrm{CUT}+}(\mathbf{DTIME}(T(n)))$ et par suite $x \notin \mathbb{R}_{\mathrm{Base}}(\mathbf{DTIME}(T(n)))$.
Pour chaque β, nous cherchons maintenant à démontrer que la suite $n \mapsto [\beta^n x]$ (où $n \in \mathbb{N}_1$) est dans $\mathbf{DTIME}(\mathrm{O}(n^{1+}))$.

Soit k_0 un entier tel que $p_{k_0} > \beta$, soit n_0 tel que $U(k_0) \leqslant 3+3n_0$. Pour $n \geqslant n_0$, nous cherchons l'entier $k \in \mathbb{N}_1$ tel que $U(k) \leqslant 3+3n < U(k+1)$ ce qui coûte $\mathrm{O}(n)$ (d'après le Lemme 2). Le dénominateur D_k de d_k est majoré par $p_k^{2U(k)}$. On a

$$2\beta^n \cdot D_k \leqslant 2\beta^n \cdot p_k^{2U(k)} < p_k^{1+n+2U(k)} < p_k^{U(k+1)/3+2U(k)} < p_k^{U(k+1)} \leqslant p_{k+1}^{U(k+1)}.$$

On a aussi la majoration:

$$|x - d_{k(n)}| \leqslant \frac{2}{p_{k+1}^{U(k+1)}},$$

et par suite

$$|\beta^n x - \beta^n d_{k(n)}| \leqslant \frac{2\beta^n}{p_{k+1}^{U(k+1)}} < \frac{1}{D_k}.$$

Donc: $[\beta^n x] = [\beta^n d_{k(n)}]$ puisque $\beta^n d_{k(n)}$ n'est pas entier et que son dénominateur est majoré par D_k.

La liste des triplets $(2\chi_{\mathscr{A}}(i)-1, p_i, U(i))$ pour $i=0,1,\ldots,k(n)$ est calculée en temps $\mathrm{O}(n)$. Si on écrit $\beta^n d_{k(n)}$ sous forme d'une formule à évaluer dans $\mathbb{Q}$ et ne contenant que des entiers (β et les p_i) et les 4 opérations arithmétiques, cela occupera donc une taille $\mathrm{O}(n^{1+})$ et demandera un temps analogue. Enfin, l'évaluation d'une telle formule, puis le calcul de la partie entière du rationnel obtenu, si on utilise les techniques de multiplication rapide, est dans $\mathbf{DTIME}(\mathrm{O}(n^{2+}))$. $\square$

Remarque 3. Le Théorème 2 peut s'interpréter en disant qu'une constante cachée dans le O de $\mathbb{R}_{\mathrm{Base}2,\beta}(\mathbf{DTIME}(\mathrm{O}(n^{2+}))$ dépend de β et n'est pas calculable en temps $S(n)$ à partir de β.

4. Suites de faible complexité ayant pour image une suite non-récursive

Nous utilisons, comme dans [3], des suites récursives de faible complexité dans $\mathbb{R}_{\text{CONV}}$, formées de réels tous rationnels, mais qui ne sont pourtant pas des suites récursives dans $\mathbb{Q}$. Soit $(u_i)_{i\in\mathbb{N}_1}:\mathbb{N}_1\to\mathbb{N}_1$ une suite **LINTIME** ayant pour image une partie $\mathscr{U}$ récursivement énumérable mais non récursive de $\mathbb{N}_1$.

On définit:

$$\omega(j,n):=\begin{cases}1 & \text{si } j \text{ est le premier entier } i \text{ vérifiant } u_i=n,\\ 0 & \text{sinon.}\end{cases}$$

Il est clair que $\omega:\mathbb{N}_1\times\mathbb{N}_1\to\mathbb{Q}$ est dans $\mathbf{DTIME}(\mathrm{O}(n^2))$.
On obtient alors:

Théorème 3. *S'il existe un facteur premier p de β qui ne divise pas β', alors il existe une* $\mathbf{DTIME}(\mathrm{O}(n^2))$*-suite dans $\mathbb{R}_{\text{Base}2,\beta'}$ qui n'est pas récursive dans $\mathbb{R}_{\text{Base}2,\beta}$.*

Preuve. Soit

$$x_n=\sum_{i=2}^{\infty}\frac{\omega(i,n)}{p^i}.$$

Notons que $x_n=0$ si $n\notin\mathscr{U}$ et $x_n=1/p^j$ si j est le premier i vérifiant $u_i=n$. Considérons la suite $(y_n)_{n\in\mathbb{N}_1}$ définie par $y_n=1/p-x_n$; on a

$$[py_n]=1 \Leftrightarrow [py_n]\geqslant 1 \Leftrightarrow y_n\geqslant\frac{1}{p} \Leftrightarrow x_n=0 \Leftrightarrow n\notin\mathscr{U}.$$

Ce test n'est pas récursif, donc (y_n) n'est pas une suite récursive dans $\mathbb{R}_{\text{Base}2,\beta}$. Montrons maintenant que (y_n) est une $\mathbf{DTIME}(\mathrm{O}(n^2))$-suite dans $\mathbb{R}_{\text{Base}2,\beta'}$. On veut calculer: $[\beta'^m y_n]$ pour les entiers m et n en unaire donnés en entrée. Soit i tel que $p^i>\beta'^m$ et on calcule $u(2),\ldots,u(i)$ en temps $\mathrm{O}((m+n)^2)$, ceci nous donne $\omega(2,n),\ldots,\omega(i,n)$, ce qui permet de conclure que:

$$x_n=\frac{1}{p^j}\quad (j\leqslant i)\quad \text{ou}\quad 0\leqslant x_n\leqslant\frac{1}{p^{i+1}}.$$

Dans le premier cas:

$$[\beta'^m y_n]=\left[\beta'^m\left(\frac{1}{p}-\frac{1}{p^j}\right)\right].$$

Dans le deuxième cas, on a

$$\frac{1}{p}-\frac{1}{p^{i+1}}\leqslant\frac{1}{p}-x_n=y_n\leqslant\frac{1}{p},$$

par suite

$$\frac{\beta'^m}{p}-\frac{1}{p}<\frac{\beta'^m}{p}-\frac{\beta'^m}{p^{i+1}}\leqslant\beta'^m y_n\leqslant\frac{\beta'^m}{p}.$$

Or $\beta'^m/p\notin\mathbb{Z}$, donc $[\beta'^m y_n]=[\beta'^m/p]$. □

Théorème 4 (non-constructif). *Il existe une suite qui est* **DTIME**$(\mathrm{O}(n^2))$ *dans chaque* $\mathbb{R}_{\mathrm{Base}2,\beta}$ *mais qui n'est pas récursive dans* $\mathbb{R}_{\mathrm{Base}}$.

Preuve. Soit

$$x_n=\sum_{i=2}^{\infty}\frac{\omega(i,n)}{p_n^i},$$

où (p_n) est une suite croissante (au sens large) **LINTIME** de nombres premiers tendant vers l'infini.

Notons que $x_n=0$ si $n\notin\mathcal{U}$ et $x_n=1/p_n^j$ si j est le premier i vérifiant $u_i=n$. Considérons la suite $(y_n)_{n\in\mathbb{N}_1}$ définie par $y_n=1/p_n-x_n$. On a

$$[p_ny_n]=1 \Leftrightarrow [p_ny_n]\geqslant 1 \Leftrightarrow y_n\geqslant 1/p_n \Leftrightarrow x_n=0 \Leftrightarrow n\notin\mathcal{U}$$

et ce test n'est pas récursif, donc la suite (y_n) n'est pas récursive dans $\mathbb{R}_{\mathrm{Base}}$.

Soit k tel que $p_k>\beta$, alors la suite double $(m,n)\mapsto[\beta^m y_{n+k}]$ est une **DTIME**$(\mathrm{O}(n^2))$ (même raisonnement que pour $[\beta'^m y_n]$ au Théorème 3).

Par ailleurs $y_1,\dots,y_k$ est une suite finie de rationnels. Donc les suites $[\beta^m y_1],\dots,[\beta^m y_k]$ sont **LINTIME**.

Mais la fonction qui associe à chaque β la suite $y_1,\dots,y_k$ dans $\mathbb{Q}$ n'est pas récursive. Et la preuve n'est donc pas constructive. □

Remerciement

Nous remercions le rapporteur pour ses remarques sur la première version de l'article.

Références

[1] J. Balcàzar, J. Diaz and J. Gabarró, *Structural Complexity I* (Springer, Berlin, 1988).
[2] K.-I. Ko, On the definition of some complexity classes of real numbers, *Math. Systems Theory* **16** (1983) 95–109.
[3] S. Labhalla and H. Lombardi, Real numbers, continued fractions, and complexity classes. *Ann. Pure Appl. Logic* **50** (1990) 1–28. La version française est de 1988.
[4] A. Mostowski, On computable sequences, *Fund. Math.* **44** (1957) 37–51.
[5] R. Rice, Recursive real numbers, *Proc. Amer. Math. Soc.* **5** (1954) 784–791.
[6] E. Specker, Nicht Konstructive beweisbare Saltze der analysis, *J. Symbolic Logic* **14** (1949) 145–158.
[7] A.M. Turing, On computable numbers, with an application to the Entscheidungs problem, *Proc. London Math. Soc.* **42** (1937) 230–265.